THE EPISCOPAL CHURCH OF THE REDEEMER

2944 Erie Avenue, Cincinnati, OH 45208 • 513-321-6700

Mary Jo Schottelkotte, Parish Office Administrator • maryjo@redeemer-cincy.org

Notice of Data Breach

November 6, 2020

«AddressBlock»

Dear «GreetingLine»:

We are contacting you regarding an incident involving certain information we maintain about you. While we have no evidence that your information was actually used, we take this event very seriously and we feel it is important to inform you of what happened, what we have done in response and what you can do to protect yourself. Please read this letter carefully and contact us with any questions as instructed below.

What Happened

On or about September 23, 2020, we discovered that certain files on our internal computer systems appeared to be inaccessible. After investigation, we determined that an intruder gained access to our systems and placed malicious code (or "malware") that blocked our access to certain files as part of what is commonly known as a ransomware attack. Our investigation revealed that the intrusion began on or about September 17, 2020 and ended on or about September 23, 2020. During that period, the intruder may have gained access to the information contained on our systems. We have engaged a forensics firm to determine whether and to what extent information may have accessed or acquired in the incident.

Our investigation has determined the information potentially exposed in the data incident contained personal information relating to you. As of now we have no evidence that the intruder used or disseminated your information or that obtaining such information was the reason for the intrusion.

What Information Was Involved

While the type of information stored on our systems varied from person to person, the information generally included some combination of name, driver's license number or other identification number, financial account number, contact information, date of birth, health information, insurance policy information, login information and social security number. Please call the phone number at the end of this letter if you have any questions regarding what types of personal information may have been involved in this matter.

What We Are Doing

To appropriately manage the incident and its impact on our organization, we consulted legal counsel and engaged outside experts experienced in handling these types of incidents to help determine the impact to our members and appropriately notify them. To prevent similar occurrences from happening in the future, we are working with a cybersecurity firm and have removed the malware from our systems and employed enhanced security controls to actively monitor our network against this type of threat. We are planning user training of our staff and volunteers on best practices for cyber security protocol.

We have not delayed this notification as a result of a law enforcement investigation.

What You Can Do

We encourage you to take preventative measures now to help prevent and detect any misuse of your information such as placing a fraud alert and/or security freeze on your credit file, performing a review of your credit reports, and enrolling in free credit monitoring services.

A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. As soon as one credit reporting agency confirms your fraud alert, the other major agencies are notified to place similar fraud alerts on your credit file. You may also decide to request a security freeze, which prevents a credit reporting agency from releasing your credit report without your consent. You may contact any one of the three major credit reporting agencies or the Federal Trade Commission to obtain additional information about fraud alerts and/or security freezes.

You are entitled to one free copy of your credit report every 12 months from each of the three major credit reporting agencies. We recommend you closely monitor your financial accounts and credit reports for incidents of fraud and identify theft, and, if you see any unauthorized activity, promptly contact your financial institution.

Equifax	Experian	Trans Union
(www.equifax.com)	(www.experian.com)	(www.transunion.com)
P.O. Box 740241 Atlanta, GA 30374-0241 1-800-685-1111	P.O. Box 2390 Allen, TX 75013 1-888-397-3742	P.O. Box 1000 Chester, PA 19016 1-800-888-4213

In addition, we are offering you identity monitoring services for 24 months, which we will provide at no cost to you. Your identity monitoring services include Consumer Identity Monitoring, Fraud Consultation and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services

You must activate your identity monitoring services by **February 6, 2021**. Your Activation Code will not work after this date.

1. Visit **https://enroll.idheadquarters.com/redeem** to activate your identity monitoring services.
2. Provide Your Activation Code: **<<Enter Activation Code>>** and Your Verification ID: **SF-002340**

To sign in to your account after you have activated your identity monitoring services, please **https://login.idheadquarters.com/**.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you remain vigilant for incidents of fraud or identity theft by checking your credit reports and account statements periodically. Checking these documents periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, you should take action. Such action may include contacting the credit reporting agencies and your financial institution(s), contacting law enforcement, including your state's attorney general and the Federal Trade Commission, and filing a police report. You should get a copy of the report since many creditors want the information it contains to resolve fraudulent debts. You also may file a complaint with the FTC.

For More Information

Additionally, the FTC offers consumer assistance and educational materials relating to steps individuals can take to avoid identity theft and privacy issues. The FTC may be contacted at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) 382-4357
www.ftc.gov/idtheft

If you have any questions about this notification or require further assistance, please feel free to contact us Monday through Friday from 9:00 a.m. to 4:00 p.m. Eastern Time at (513) 800-1452.

Sincerely,

Mary Jo Schottelkotte
Parish Administrator
THE EPISCOPAL CHURCH OF THE REDEEMER
2944 Erie Avenue, Cincinnati, OH 45208 • 513-321-6700
www.redeemer-cincy.org